UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,579	09/26/2004	Amiram Grynberg		5578

32490 7590 04/29/2008

AMIRAM GRYNBERG
24 RIMON ST
NEVE EFRAYIM MONSON, 60190
ISRAEL

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/711,579	GRYNBERG, AMIRAM	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on Sep. 26, 2004.

2. Claims 1-13 are under examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 5-7 and 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm (US Patent No. 7,333,956) and in view of Abdulhayoglu (US Pub. No. 2004/0078564).

As per claim 1, Malcolm teaches:

detecting form data before a form is submitted to a target site; accessing said form data; detecting sensitive form fields within said form data **[*col. 9 lines 43-67, col. 10 1-24, 35-46 Fig. 6, col. 10 lines 58-65*, "...the potentially sensitive user data is transmitted to the web site via the web server when the user selects a `Submit` button. At this stage, the BHO can trap the `Submit` event issued by the web browser, and access the DOM to extract the user data"**, Fig. 18, ***col. 14 lines 46-51*** **"a username or a password is detected by the plug-in module at step S152 then control passes to step S154, where the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted"]**; analyzing URL of said target site against security criteria to generate an alert code; matching said alert code

with blocking criteria to generate a match condition; blocking submission of said form to said target site if said match condition is generated **[*col. 14 lines 48-50*, "...the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted", *col. 24 line 67, col. 25 1-3*, "Determining whether a link is secure is achieved by examining the URL of the destination web page. A secure link is indicated by an `s` after the prefix `http`". *col. 26 lines 37-67*, The URL is compared with the various conditions and tables of the policy data as shown in Figs. 7 and 13. *col. 27 lines 42-67, col. 28 lines 1-54*. Performing a specific action based on the specified policy data, e.g. If it determines that the connection is insecure then generates the warning and terminates the transaction, Fig. 18, *col. 35 lines 12-29* "If the security of the link is not sufficient for the nature of the information being transmitted then, the module may either prevent the transmission from taking place and warn the user...."]**.

Further, Malcolm teaches analyzing certificate **[*col. 19 lines 57-67, col. 20 -1-67*, Figs. 9-10]**. Malcolm doesn't expressively mention analyzing certificate *of said target site*.

However, Abdulhayoglu teaches analyzing certificate of said target site **[*paragraph 0010,* "the web site comprises a digital certificate. Suitably, the digital certificate comprises data for displaying the hallmark. The hallmark verification process comprises the steps of verifying the digital certificates, displaying a hallmark from the digital certificate at a location and indicating the veracity of a certificate at the location to the user" *paragraph 0241-0261*, "The digital certificate includes the following dedicated information: a) the URL of the web site authorised to publish the particular hallmark; Comparing the URL contained in the certificate (see a) above) with that of the site being visited (step 108). 2) Comparing the file name, file size and**

file dimensions (see b) above) contained in the certificate with the corresponding attributes of the hallmark presented by the web site (step 110). 3) Checking the revocation date of the hallmark to ensure its validation is still current"].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Abdulhayoglu with Malcolm to analyze or verify the certificate of the web site, since one would have been motivated to provide confident to the user for transaction over the Internet and enhance the security **[Abdulhayoglu, *paragraph 0002-0006, 0105*]**.

As per claim 2, the rejection of claim 1 is incorporated and Malcolm teaches:

wherein the step of detecting sensitive form data further includes: receiving a notification message from said browsing program that form data is about to be submitted; receiving a URL of said target site together with said notification message **[*col. 10 lines 3-24, 35-64*, "The BHO is implemented to monitor navigation requests and data submitted to the web server from the browser and identify data that is unique to the user". "The BHO may search for the `?` symbol, which indicates the end of the URL address being connected to and indicates that what follows is data". "Also, the BHO may be implemented to monitor the operation of the web browser itself. As the web browser operates it generates `events` to notify co-dependent software modules or objects that something significant has just occurred or that an action has just been completed. The name of the event is usually descriptive in its own right of what has just occurred; additional data that describes the event in more detail is normally available. The BHO is implemented to trap these events and to take action in dependence on them". "Another event that the BHO traps is the `DocumentComplete` event,...", "The DOM provides**

comprehensive access to the data comprising the page, allowing the BHO to extract data items which are of interest to it". "the potentially sensitive user data is transmitted to the web site via the web server when the user selects a `Submit` button. At this stage, the BHO can trap the `Submit` event issued by the web browser, and access the DOM to extract the user data". c*ol. 14 lines 46-51* "a username or a password is detected by the plug-in module at step S152 then control passes to step S154, where the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted"].

As per claim 3, the rejection of claim 2 is incorporated and Malcolm teaches:

wherein the step of analyzing said target site further includes checking *for at least one of the following attributes*: *site server being listed in saved sites database*; secure communication protocol in the URL of target site **[Fig. 13, *col. 26 lines 62-67* "the URL is compared with a list of known eCommerce URLs stored in a file or in a database. In decision step S266, a determination on that comparison is made. If the URL is found to be at a known eCommerce page, or within a known set of eCommerce pages", *col. 28 lines 28-37* "The IfKnownECommerceSite branch allows the user to specify a list of URLs corresponding to sites, parts of sites, or even single pages, where eCommerce transactions are known to take place. The current page URL is matched against entries in this list to determine if a transaction is taking place. The KnownSites sub-branch contains a reference to table s in which the URLs of known eCommerce sites are stored", *col. 25 lines 1-5* "Determining whether a link is secure is**

achieved by examining the URL of the destination web page. A secure link is indicated by an `s` after the prefix `http`"].

Abdulhayoglu teaches: checking a valid site server certificate **[*paragraph 0010*, "The hallmark verification process comprises the steps of verifying the digital certificates, displaying a hallmark from the digital certificate at a location and indicating the veracity of a certificate at the location to the user"** ***paragraph 0241-0261*****, "The digital certificate includes the following dedicated information: a) the URL of the web site authorised to publish the particular hallmark; Comparing the URL contained in the certificate (see a) above) with that of the site being visited (step 108). 2) Comparing the file name, file size and file dimensions (see b) above) contained in the certificate with the corresponding attributes of the hallmark presented by the web site (step 110). 3) Checking the revocation date of the hallmark to ensure its validation is still current"].**

As per claim 5, the rejection of claim 3 is incorporated and Malcolm teaches:

wherein preset security triggers are determined by an automated policy and the steps of matching analysis results with blocking criteria further include: comparing generated alert code with rules specified in an a policy; generating a match condition *if at least one policy rule matches* said alert code **[Fig. 7, 13,** ***col. 15 lines 23-62, col. 17 lines 28-35, 47-55*****, "...the credit card number, and other details of the transaction are compared to the settings in the policy file and it is determined whether or not transmission may take place. If for any reason, with reference to the policy checks, it is determined that the credit card number should not be transmitted, control passes to step S172 where transmission of the data is halted, and then to step S174**

where the module exits. At this point the system could notify the user that the request has been denied by means of a pop-up message box...", *col. 27 lines 42-67, col. 28 lines 1-54*. "...the policy data used to identify that eCommerce transaction is occurring and to control the way in which the transaction data is recorded. The policy data is represented by a Transactions branch of the policy data tree which sub-divides into two separate sub-branches called "Identification" and "Termination". The Identification branch is itself divided into five sub-branches which correspond to the determinations made in the process illustrated in FIG. 12". "The IfKnownECommerceSite branch allows the user to specify a list of URLs corresponding to sites, parts of sites, or even single pages, where eCommerce transactions are known to take place. The current page URL is matched against entries in this list to determine if a transaction is taking place. The KnownSites sub-branch contains a reference to table s in which the URLs of known eCommerce sites are stored. The determination of whether the URL of the web site is a known eCommerce site is made in decision step S266 following step S264 of FIG. 12". "The Termination branch of the Transactions branch divides into four sub-branches which specify conditions which are used to end the recording of data being transmitted or received. Each sub-branch sets out a condition by which the end of the transaction may be defined. The first branch entitled "IfConnectionGoesInsecure" allows a user to specify that the relinquishing of a secure connection by the web browser indicates the end of a transaction". (i.e. comparing the various conditions with the specified rules of the policy data and performing the action based on the policy data). Fig. 18].

As per claim 6, the rejection of claim 1 is incorporated and Malcolm teaches:

wherein the step of detecting form data further includes: detecting a network login dialog window containing at least a password field; retrieving a URL of said target site from a browsing program **[*col. 10 lines 50-64, col. 14 lines 46-51*, "a username or a password is detected by the plug-in module at step S152 then control passes to step S154, where the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted"]**.

As per claim 7, the rejection of claim 6 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 9, the rejection of claim 7 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 10, Malcolm teaches:

A system for blocking submission of online forms, comprising a computing device with access to a network, a first browsing program adapted to be executed on said device and a second monitoring program adapted to be executed on said device configured to **[Fig. 1]**: accept notifications from said browsing program before a form is submitted to a target site; access form data in said browsing program and detect form fields of a sensitive nature; retrieve from said browsing program a URL of said target site **[*col. 9 lines 43-67, col. 10 1-24, 35-46* Fig. 6, *col. 10 lines 58-65*, "...the potentially sensitive user data is transmitted to the web site via the web server when the user selects a `Submit` button. At this stage, the BHO can trap the `Submit` event issued by the web**

browser, and access the DOM to extract the user data", **Fig. 18,** ***col. 14 lines 46-51*** **"a username or a password is detected by the plug-in module at step S152 then control passes to step S154, where the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted" col. 10 lines 3-24, 35-64]**; analyze URL of said target site against security criteria to generate an alert code; match said alert code with blocking criteria to generate a match condition; block submission of said online form to said target site if said match condition is generated **[*col. 14 lines 48-50*, "...the values of the identified username or password and the URL or other identifier of the web page to which the data is to be transmitted are extracted",** ***col. 24 line 67, col. 25 1-3*****, "Determining whether a link is secure is achieved by examining the URL of the destination web page. A secure link is indicated by an `s` after the prefix `http`".** ***col. 26 lines 37-67*****, The URL is compared with the various conditions and tables of the policy data as shown in Figs. 7 and 13.** ***col. 27 lines 42-67, col. 28 lines 1-54*****. Performing a specific action based on the specified policy data, e.g. If it determines that the connection is insecure then generates the warning and terminates the transaction, Fig. 18,** ***col. 35 lines 12-29*** **"If the security of the link is not sufficient for the nature of the information being transmitted then, the module may either prevent the transmission from taking place and warn the user...."]**.

Further, Malcolm teaches analyzing certificate **[*col. 19 lines 57-67, col. 20 -1-67*, Figs. 9-10]**. Malcolm doesn't expressively mention analyzing certificate *of said target site*.

However, Abdulhayoglu teaches analyzing certificate of said target site **[*paragraph 0010*, "the web site comprises a digital certificate. Suitably, the digital certificate comprises data for displaying the hallmark. The hallmark verification process comprises the steps of verifying the**

digital certificates, displaying a hallmark from the digital certificate at a location and indicating the veracity of a certificate at the location to the user" *paragraph 0241-0261*, "The digital certificate includes the following dedicated information: a) the URL of the web site authorised to publish the particular hallmark; Comparing the URL contained in the certificate (see a) above) with that of the site being visited (step 108). 2) Comparing the file name, file size and file dimensions (see b) above) contained in the certificate with the corresponding attributes of the hallmark presented by the web site (step 110). 3) Checking the revocation date of the hallmark to ensure its validation is still current"].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Abdulhayoglu with Malcolm to analyze or verify the certificate of the web site, since one would have been motivated to provide confident to the user for transaction over the Internet and enhance the security **[Abdulhayoglu, *paragraph 0002-0006, 0105*]**.

As per claim 11, the rejection of claim 10 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 12, the rejection of claim 11 is incorporated and Malcolm teaches:

where said monitoring program is part of a password management program adapted to be executed on said device **[*col. 13 lines 60-67, col. 14 lines 1-41, col. 15 lines 13-22* "The plug-in modules provided by the preferred system operate in conjunction with policy data, which may be recorded in a file, database, or software code for example. The policy data provides a user of**

the preferred system to instruct the operation of each of the plug-in modules thereby controlling their functionality. A sample representation of policy data, illustrated in FIG. 7, shows how a user may control the operation of the plug-in module to record password and username information along with other types of data"].

As per claim 13, the rejection of claim 11 is incorporated and Malcolm teaches:

wherein said monitoring program is an integrated part of said browsing program **[*col. 9 lines 63-67, col. 10 lines 1-57*, "The plug-in module provided by the preferred embodiment of the invention in the form of a Browser Helper Object (BHO) provides additional functionality to augment that of the standard web browser. The BHO is implemented to respond to a number of significant events that occur as the web browser is operated and directed by the user to interact with various web sites and pages"].**

4. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malcolm (US Patent No. 7,333,956) in view of Abdulhayoglu (US Pub. No. 2004/0078564) and in view of Toomey (US Patent No. 7,152,244).

As per claim 4, the rejection of claim 3 is incorporated and Malcolm teaches:

wherein blocking criteria are determined by a user and the steps of matching alert codes with blocking criteria further include: inputting by said user a list of alert codes which should cause an alert **[Fig. 7, *col. 15 lines 19-22*, "A sample representation of policy data, illustrated in FIG. 7, shows**

how a user may control the operation of the plug-in module to record password and username information along with other types of data", *col. 28 lines 60-67*, "policy data shown in this diagram, in particular, but also in the other diagrams is unique to each user. Not only may a user specify whether or not particular conditions are to be acted on by setting the Yes or No variable accordingly, or by changing the number of pages that are to be recorded for example, but also the structure and arrangement of branches and conditions specified on those branches may be different from user to user", Fig. 13, *col. 27 lines 45-59, col. 28 lines 47-55*]; generating a physical alert if any of analysis results match *at least one entry* in said list; presenting to said user said physical alert **[Fig. 18, *col. 35 lines 26-29*, "...If the security of the link is not sufficient for the nature of the information being transmitted then, the module may either prevent the transmission from taking place and warn the user"].**

Malcolm teaches presenting pop-up message box (warning or physical alert) to the user **[*col. 17 lines 47-55, col. 28 lines 47-55*]**. Malcolm and Abdulhayoglu don't expressively mention *accepting enable/disable submission input* from said user.

However, Toomey teaches: accepting enable/disable submission input from said user; generating a match condition if a disable input is received from said user (and blocking submission of said form to said target site) **[Fig. 2D, 2E, 3C, *col. 16 lines 26-53*, "...the form is not from a known, trusted website, the context is considered unsafe. As a result, a warning dialog 360 is displayed to the employee to warn the employee that submitting his or her security credentials to this website may be unsafe. Dialog 360 includes text 365 that warns the employee that his or her security credentials should not be submitted to a website unless the employee completely trusts the website. Text 365 also requests the employee to confirm whether or not he or she**

wants to continue. A "Yes" button 375 is provided for the employee to confirm that he or she wants to continue. Selecting Yes button 375 results in dialog 360 closing and the employee being allowed to submit the credentials by selecting submit button 355. A "No" button 380 is provided for the employee to indicate he or she does not want the credentials submitted. Selecting the No button 380 results in the employee being prevented from submitting the credentials. He or she may be prevented, for example, by clearing the entries in textfields 340 and 345 and disabling the submit button 355, or otherwise preventing communications with the website"].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods of Malcolm and Abdulhayoglu by including the step of Toomey because it would provide protection against a computer user unintentionally giving away sensitive data to an illegitimate or unintended entity **[Toomey, *col. 2 lines 16-18*]**.

As per claim 8, the rejection of claim 7 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shraim et al (US 2007/0299915) – Customer-based detection of online fraud

Shraim et al (US 2007/0294352) – Generating phish message

Brinson et al (US 2006/0080735) – Method and system for phishing detection and notification

Page (US 2007/0124270) – System and methods for an identity theft protection bot

Bantz et al (US 7313691) – Internet site authentication service

Brown et al (US 2003/0037138) – Method, apparatus and program for identifying, restricting and monitoring data sent from client computers

Sidles (US 2002/0062342) – Method and system for completing forms on wide area networks such as the internet

Dutta (US 7089582) – Method and apparatus for identifying universal resource locator rewriting in a distributed data processing system

Korn et al (US 6442607) – Controlling data transmission from a computer

WO 2006/036170 – Method and System for filtering URLS, WebPages, and Content

Groshon et al (US 6351811) – System and method for preventing transmission of compromised data in a computer network

Bryant (US 6286046) – Method of recording and measuring e-business session on the world wide web

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
3/5/08
/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135